

bitdefender[®]

ANTIVIRUS FOR MAC

User's Guide



BitDefender Antivirus for Mac

BitDefender Antivirus for Mac *User's Guide*

Publication date 2010.11.29

Copyright© 2010 BitDefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of BitDefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of BitDefender, therefore BitDefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. BitDefender provides these links only as a convenience, and the inclusion of the link does not imply that BitDefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

Preface	vi
1. Book Structure	vi
2. Conventions Used in This Book	vii
2.1. Typographical Conventions	vii
2.2. Admonitions	vii
3. Request for Comments	viii
1. Installation and Removal	1
1.1. System Requirements	1
1.2. Installing BitDefender Antivirus for Mac	2
1.2.1. Step 1 - Welcome Window	3
1.2.2. Step 2 - View the Readme File	4
1.2.3. Step 3 - Read the License Agreement	5
1.2.4. Step 4 - Start Installation	6
1.2.5. Step 5 - Installing BitDefender	7
1.2.6. Step 6 - Finish	8
1.3. Removing BitDefender Antivirus for Mac	9
2. Getting Started	11
2.1. About BitDefender Antivirus for Mac	11
2.2. How BitDefender Antivirus for Mac Protects You	12
2.3. What You Have to Do After Installation	12
2.4. Opening BitDefender Antivirus for Mac	13
2.5. Application Main Window	13
2.5.1. Toolbar	14
2.5.2. Status Area	15
2.5.3. Advanced Controls Area	17
2.5.4. Bottom Bar	18
2.6. Application Dock Icon	18
3. Protecting against Malicious Software and Phishing Scams	21
3.1. Fixing Issues	21
3.1.1. Checking Issues	22
3.1.2. Fixing Issues	23
3.2. Antiphishing Protection	24

BitDefender Antivirus for Mac

3.3. Shield	24
3.3.1. Enabling or Disabling Shield	25
3.3.2. Configuring Shield Settings	25
3.3.3. Checking Shield Activity	28
3.4. Scanner	28
3.4.1. Scanning Your Mac	29
3.4.2. Scan Wizard	31
3.4.3. Checking Scan Logs	34
3.4.4. Setting Up Scheduled Scans	35
3.4.5. Configuring Scan Settings	36
3.5. Scan Exclusions	37
3.5.1. Accessing the Scan Exclusions List	38
3.5.2. Managing Scan Exclusions	39
3.6. Quarantine	40
3.6.1. Accessing Quarantined Files	40
3.6.2. Managing Quarantined Files	41
3.7. Updates	42
3.7.1. Enabling or Disabling Automatic Update	42
3.7.2. Requesting an Update	43
3.7.3. Getting Updates through a Proxy Server	43
4. Configuring Preferences	44
4.1. Accessing Preferences	44
4.2. General Preferences	44
4.3. Shield Preferences	46
4.4. Security Preferences	47
5. Registering BitDefender Antivirus for Mac	48
5.1. About Registration	48
5.2. Registering BitDefender Antivirus for Mac	48
5.3. Purchasing a License Key	49
6. Getting Help	50
6.1. Support	50
6.1.1. Online Resources	50
6.1.2. Asking for Help	52
6.2. Contact Information	52

BitDefender Antivirus for Mac

- 6.2.1. Web Addresses 53
 - 6.2.2. BitDefender Offices 53
 - 6.2.3. Local Distributors 55
- Types of Malicious Software 56
- What Is Phishing? 59

Preface

This guide is intended to all Macintosh users who have chosen **BitDefender Antivirus for Mac** as a security solution for their computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Macintosh.

This book will describe for you BitDefender Antivirus for Mac, will guide you through the installation process, will teach you how to configure it. You will find out how to use BitDefender Antivirus for Mac, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Book Structure

The book consists of several chapters containing major topics.

Installation and Removal (p. 1)

Step by step instructions for installing BitDefender Antivirus for Mac on your Mac. Starting with the prerequisites for a successfully installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

Getting Started (p. 11)

Get started with BitDefender Antivirus for Mac and its user interface.

Protecting against Malicious Software and Phishing Scams (p. 21)

Learn how to use BitDefender Antivirus for Mac to protect yourself against malicious software and phishing scams.

Configuring Preferences (p. 44)

Learn more about the BitDefender Antivirus for Mac preferences.

Registering BitDefender Antivirus for Mac (p. 48)

Find out how to register BitDefender Antivirus for Mac and buy a license key.

Getting Help (p. 50)

Where to look and where to ask for help if something unexpected appears.

2. Conventions Used in This Book

2.1. Typographical Conventions

Several text styles are used in the book for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
<code>sample syntax</code>	Syntax samples are printed with monospaced characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
sales@bitdefender.com	E-mail addresses are inserted in the text for contact information.
<i>Preface (p. vi)</i>	This is an internal link, towards some location inside the document.
<code>filename</code>	File and directories are printed using monospaced font.
option	All the product options are printed using bold characters.
keyword	Important keywords or phrases are highlighted using bold characters.

2.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.



Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.



Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.



Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

3. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to documentation@bitdefender.com.



Important

Please write all of your documentation-related e-mails in English so that we can process them efficiently.

1. Installation and Removal

This chapter includes the following topics:

- *System Requirements* (p. 1)
- *Installing BitDefender Antivirus for Mac* (p. 2)
- *Removing BitDefender Antivirus for Mac* (p. 9)

1.1. System Requirements

You may install BitDefender Antivirus for Mac only on Intel-based Macintosh computers with Mac OS X version 10.4.6 or later installed.

Your Mac must also meet all of these additional requirements:

- Minimum 1 GB of RAM Memory
- Minimum 200 MB available hard disk space
- Display colors: millions.
- Minimum normal (4:3) display resolution: 1024 x 768
- Minimum wide display resolution: 1024 x 640

An Internet connection is required to register and update BitDefender Antivirus for Mac.

Antiphishing protection is only available for Mac OS X version 10.5 or later with:

- Safari 5.0.1 (or higher)
- Firefox 3.5 (or higher)

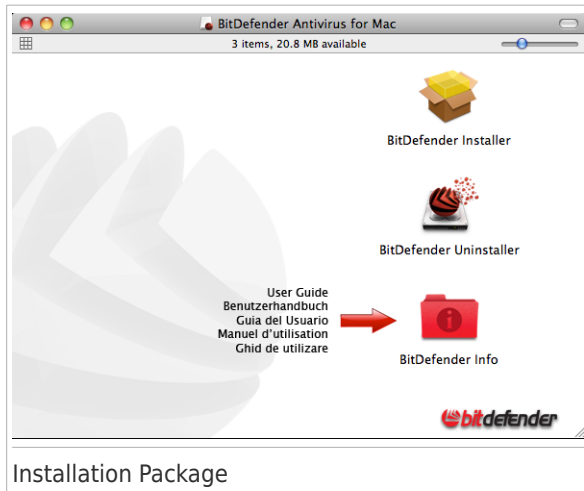


How to find out your Mac OS X version and hardware information about your Mac

Click the Apple icon in the upper-left corner of the screen and choose **About This Mac**. In the window that appears you can see the version of your operating system and other useful information. Click **More Info** for detailed hardware information.

1.2. Installing BitDefender Antivirus for Mac

Locate the `bitdefender.dmg` file and double-click it. The following window will appear.



Click `BitDefenderInstaller.pkg`. This will launch the installer, which will guide you through the installation process.

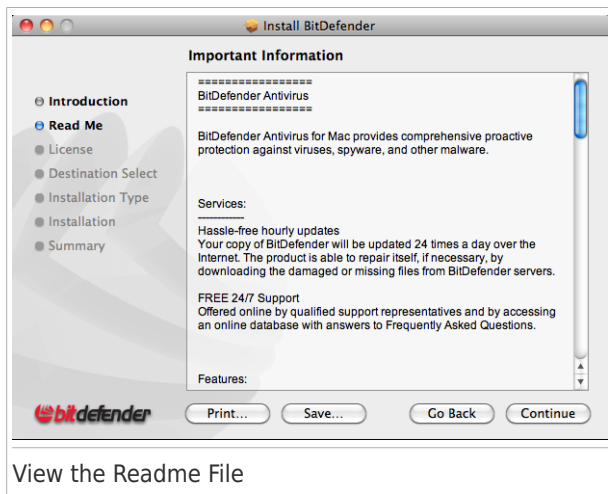
BitDefender Antivirus for Mac

1.2.1. Step 1 - Welcome Window



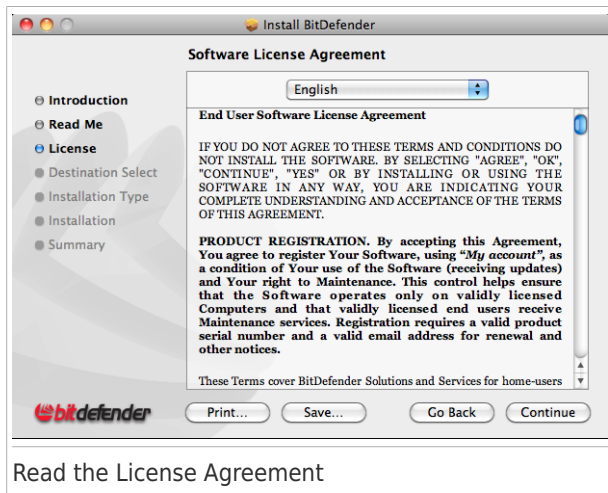
Click **Continue**.

1.2.2. Step 2 - View the Readme File



The readme file provides useful information about BitDefender Antivirus for Mac. You can print or save the readme file so that you can review it at a later time. Click **Continue**.

1.2.3. Step 3 - Read the License Agreement



The License Agreement is a legal agreement between you and BitDefender for the use of BitDefender Antivirus for Mac. You can print or save the License Agreement so that you can review it at a later time.

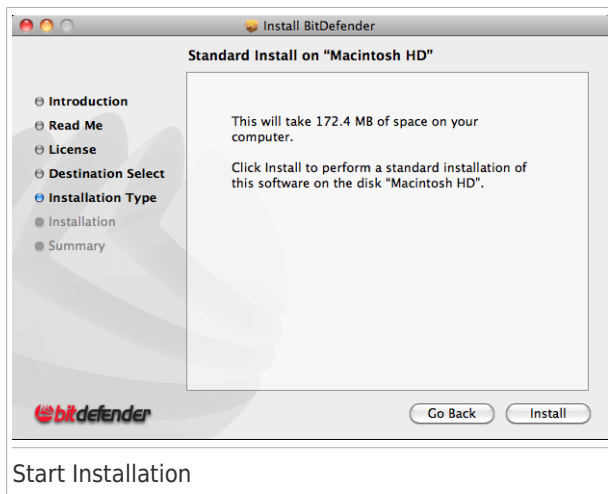
Please read the License Agreement carefully. To continue installing the software you must agree to the terms of the software license agreement. Click **Continue** and then **Agree**.



Important

If you do not agree to these terms, click **Continue** and then **Disagree** to cancel the installation and quit the installer.

1.2.4. Step 4 - Start Installation



BitDefender Antivirus for Mac will be installed in Macintosh HD/Library/BitDefender. You cannot change the installation path.

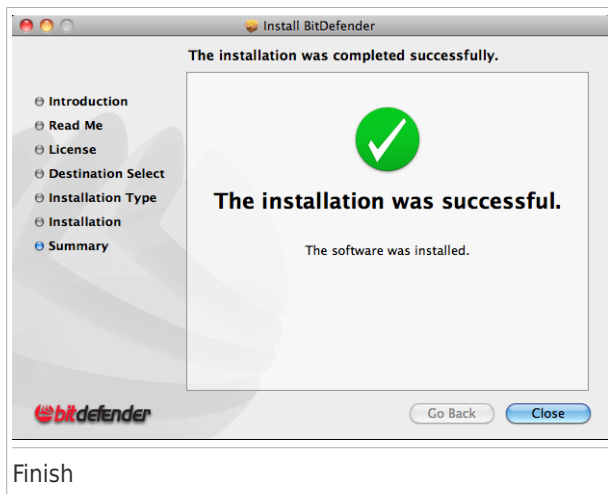
Click **Install** to start the installation.

1.2.5. Step 5 - Installing BitDefender



Wait until the installation is completed and then click **Continue**.

1.2.6. Step 6 - Finish



Click **Close** to close the installer window.

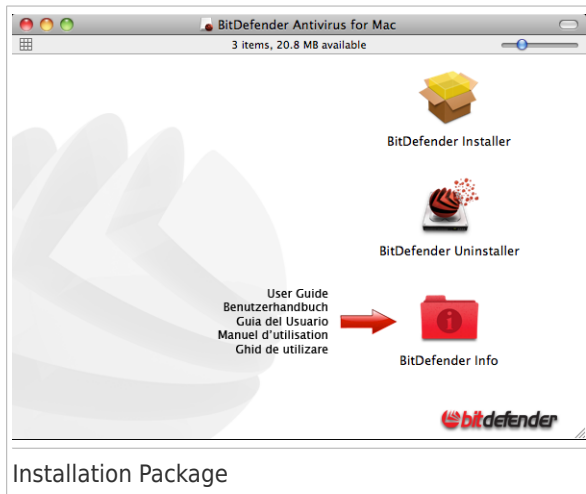
1.3. Removing BitDefender Antivirus for Mac

Being a complex application, BitDefender Antivirus for Mac cannot be removed in the normal way, by dragging the application icon from the Applications folder to the Trash.

To remove BitDefender Antivirus for Mac, you need the `bitdefender.dmg` installation file (either the original or a new one).

Follow these steps:

1. Locate the `bitdefender.dmg` file and double-click it. The following window will appear.



2. Click `BitDefenderUninstaller.pkg`. The installer will help you run the uninstall script of BitDefender Antivirus for Mac.

3. Click **Continue**.
4. Click **Install** to run the uninstall script.
5. You can see if the uninstall script was run successfully. Click **Close** to close the installer window.



Important

If there is an error, you can contact BitDefender Customer Care as described in *Support* (p. 50).

2. Getting Started

This chapter includes the following topics:

- *About BitDefender Antivirus for Mac* (p. 11)
- *How BitDefender Antivirus for Mac Protects You* (p. 12)
- *What You Have to Do After Installation* (p. 12)
- *Opening BitDefender Antivirus for Mac* (p. 13)
- *Application Main Window* (p. 13)
- *Application Dock Icon* (p. 18)

2.1. About BitDefender Antivirus for Mac

BitDefender Antivirus for Mac is a complete antivirus solution, which protects against all kinds of malicious software ("malware"), including:

- viruses
- spyware
- Trojan horses
- keyloggers
- worms
- adware

Moreover, you can be sure that the files you send to friends using Windows operating systems cannot infect their PC.

Besides antivirus protection, BitDefender Antivirus for Mac also provides protection against online phishing scams. These are attempts to steal personal or financial information (for example, user names and passwords, credit card numbers), using a forged web site, with the purpose of making profits or obtaining other benefits.

2.2. How BitDefender Antivirus for Mac Protects You

BitDefender Antivirus for Mac includes the following protection features:

- **Shield** - automatically checks the files that you open, copy or download for malicious software.
- **Scanner** - allows you to check your system for malicious software whenever you want and to remove detected threats. You can set up scheduled scans to create automatic scanning routines. For example, you can set an automatic full-system scan, which is recommended by BitDefender for greater protection.
- **Antiphishing** - blocks access to web pages set up to steal personal information (for example, user names and passwords, credit card numbers).

Moreover, BitDefender Antivirus for Mac automatically updates its malware signatures **every hour**. In this way, you are protected against the latest malware threats identified by the BitDefender Labs.

2.3. What You Have to Do After Installation

Once you have installed BitDefender Antivirus for Mac, you are automatically protected against malicious software and phishing scams. However, there are a few things you have to do to maintain and enhance your protection.

- Immediately after the installation, scan your system to make sure it is clean. To this purpose, run a full system scan. If malware is found, the infected files will be automatically cleaned or isolated in quarantine. To find out how to start a scan, refer to *Scanning Your Mac* (p. 29).
- For greater protection, it is recommended that you scan your system regularly, at least once a week. The most convenient way to do this is to set up a scheduled scan. For more information, refer to *Setting Up Scheduled Scans* (p. 35).
- To maintain your protection, you must register your copy of BitDefender Antivirus for Mac within 30 days after installation. For more information, refer to *Registering BitDefender Antivirus for Mac* (p. 48).

BitDefender Antivirus for Mac

- Check and fix the issues reported by BitDefender Antivirus for Mac regularly. For detailed information, refer to *Fixing Issues* (p. 21).

No other configuration or action is required. However, if you want to, you can adjust the application settings and preferences to better suit your needs. For more information, refer to *Configuring Preferences* (p. 44).

2.4. Opening BitDefender Antivirus for Mac

You can open BitDefender Antivirus for Mac to check the system security status, take preventive measures to protect against malware or set up the application.

You have several ways to open BitDefender Antivirus for Mac.

- Click the BitDefender icon in the Dock.
- Open a Finder window, go to **Applications** and double-click the BitDefender alias (or right-click it and choose **Open**).

Alternatively, you can use Spotlight to find and open the application.

- Open a Finder window, go to **Macintosh HD** → **Library** → **BitDefender** → **AVP** and double-click BitDefender (or right-click it and choose **Open**).



Note

The application alias in **Applications** and the application icon in the Dock are removable. If you do not find them, use the third method to open the application.

2.5. Application Main Window

In the application's main window you can check your computer's security status, fix security issues, start scans and configure security settings.

BitDefender Antivirus for Mac



Application Main Window

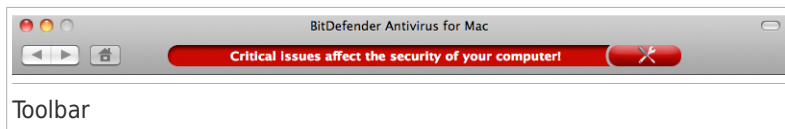
The main window is divided into four areas:

- a toolbar at the top of the window
- the status area
- the advanced controls area
- the bottom bar

2.5.1. Toolbar

The toolbar at the top of the window helps you navigate through the application and fix security issues.

BitDefender Antivirus for Mac



The toolbar contains navigation buttons, a status bar and a button you can use to fix issues (if any).


The following intuitive navigation buttons are available:

-  **Back**
-  **Forward**
-  **Home**



Note

You can use keyboard shortcuts to navigate through the application. Open the View application menu to see the available keyboard shortcuts.

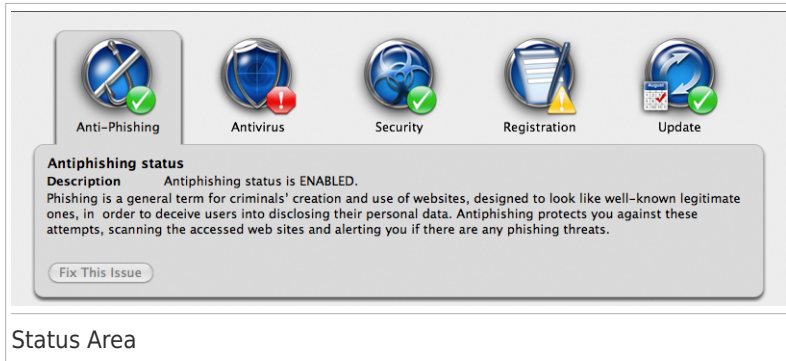
The status bar informs you about the system's security status using explicit messages and suggestive colors. If all of the monitored security parameters are OK, the status bar is green. Otherwise, it changes its color to red if critical security issues are detected and to yellow for medium security risk. If there are any issues, a yellow or red **Fix All Issues** button () helps you fix them.

For detailed information on issues and how to fix them, refer to [Fixing Issues \(p. 21\)](#).

2.5.2. Status Area

The status area informs you about and helps you fix security risks systematically, by dividing them into several categories of interest.

BitDefender Antivirus for Mac



The following status buttons are available:

- **Antiphishing** - informs you about the antiphishing protection status and helps you fix the related issues.
- **Antivirus** - informs you about the real-time antivirus protection status and helps you fix issues related to your antivirus protection.
- **Security** - informs you about and helps you remove the existing threats.
- **Registration** - informs you about your registration status and helps you fix the related issues.
- **Update** - informs you about the update status and helps you fix the related issues.

You can easily see if there are issues that might affect your computer. Each status button is marked with an icon that indicates the current security status. This is what each icon means:

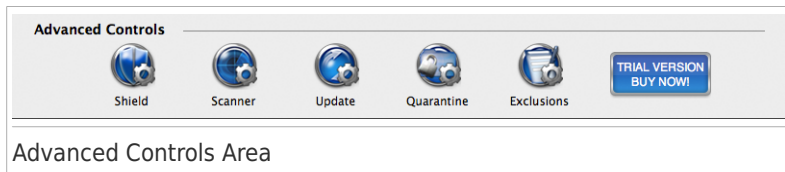
❗ **Red hexagon with an exclamation mark:** Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.

⚠ **Yellow triangle with an exclamation mark:** Minor issues affect the security of your system. You should check and fix them when you have the time.

✅ **Green circle with a check mark:** No issues have been detected.

2.5.3. Advanced Controls Area

The advanced controls area allows you to adjust the security controls, start scans and updates, manage quarantined files and scan exclusions, and check the activity of BitDefender Antivirus for Mac.

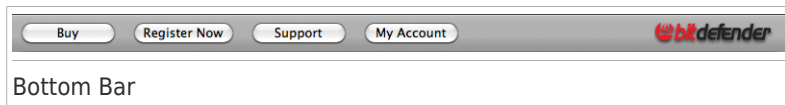


The following buttons are available:

- **Shield** - to access the advanced controls and statistics related to real-time protection.
- **Scanner** - to manage and start scans, set up scheduled scans and check the on-demand scan logs.
- **Update** - to manage and check the application and malware signature updates.
- **Quarantine** - to view and manage the quarantined files.
- **Exclusions** - to specify files and folders that you do not want to be scanned by BitDefender.

2.5.4. Bottom Bar

The bottom bar provides several useful shortcuts.



This is what each button does:

- **Buy** - takes you to a web page where you can buy a new license key or renew your license.
- **Register Now** - opens a dialog where you can enter your license key and view registration information.
- **Support** - takes you to the BitDefender Web Self-Service page from which you can contact the BitDefender Customer Care team.
- **My Account** - takes you to a web page where you can create and login to your BitDefender account.

2.6. Application Dock Icon

By default, BitDefender Antivirus for Mac sets and keeps its icon in the Dock.

The BitDefender Antivirus for Mac icon in the Dock provides an easy way to manage protection without opening the main window.

BitDefender Antivirus for Mac



Control-click the dock icon to access its shortcut menu:

- **Fix All Issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to ***[Fixing Issues](#)*** (p. 21).
- **Enable Real-time Protection** - turns on real-time protection against malicious software.
- **Disable Real-time Protection** - turns off real-time protection against malicious software.
- **Update Now** - starts an immediate update. The update is performed in the background.

If BitDefender Antivirus for Mac is open, its Dock icon also informs you about the current security status. A red badge over the Dock icon indicates the number of critical security issues. Such issues require your immediate attention and must

be fixed as soon as possible. For detailed information, refer to *Fixing Issues* (p. 21).



Note

If there is no badge, then the application's features designed to protect your system are turned on and the recommended security tasks have run. Your Mac is safe.

3. Protecting against Malicious Software and Phishing Scams

This chapter includes the following topics:

- *Fixing Issues* (p. 21)
- *Antiphishing Protection* (p. 24)
- *Shield* (p. 24)
- *Scanner* (p. 28)
- *Scan Exclusions* (p. 37)
- *Quarantine* (p. 40)
- *Updates* (p. 42)

3.1. Fixing Issues

BitDefender Antivirus for Mac automatically detects and informs you about a series of issues that can affect the security of your system and data. In this way, you can fix security risks easily and in a timely manner, without having to be a technical genius or to spend time investigating them.

Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. They are grouped into two categories:

- **Critical issues** - prevent BitDefender Antivirus for Mac from protecting you against malware or represent a major security risk. This is the list of critical issues that are reported:
 - ▶ Unresolved threats have been detected on your system.
 - ▶ Real-time antivirus protection is turned off.
 - ▶ Antiphishing protection is turned off.


- ▶ Your system was never scanned for viruses.
- ▶ Your Mac has not been scanned for more than 6 days.
- ▶ The application and its malware signatures have not been updated for more than one day.
- ▶ The trial or licensing period for your copy of the application has ended.
- **Minor (non-critical) issues** - can affect your protection against malware in the near future. This is the list of minor issues that are reported:
 - ▶ Automatic update of BitDefender Antivirus for Mac is turned off.
 - ▶ The trial or licensing period for your copy of the application is about to expire.


3.1.1. Checking Issues

If BitDefender Antivirus for Mac is open, you can easily see if there are any critical issues by taking a look at its Dock icon. A red badge over the Dock icon indicates the number of critical security issues. Such issues require your immediate attention and must be fixed as soon as possible.

To check the detected issues:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Click each status button marked with an icon that indicates the existence of security issues. This is what each icon means:

 **Red hexagon with an exclamation mark:** Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.

 **Yellow triangle with an exclamation mark:** Minor issues affect the security of your system. You should check and fix them when you have the time.

 **Green circle with a check mark:** No issues have been detected.




3. Check the description for more information.

3.1.2. Fixing Issues

Fixing the issues indicated by BitDefender Antivirus for Mac is a quick and easy way to ensure continuous protection against malicious software and phishing scams.

You have several ways to fix the detected issues.

● Follow these steps:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Do any of the following:
 - ▶ To fix all of the issues detected, click the elliptical **Fix All Issues** button () in the upper area of the window.
 - ▶ To check and fix issues one by one, click the status buttons indicating the existence of security issues (marked with  or ) and then click the **Fix This Issue** button.

● Control-click the BitDefender Dock icon and choose **Fix All Issues**.

This is what happens when you fix issues:

- If an important security setting (for example, automatic update) is currently turned off, it will be turned on immediately.
- If the trial or licensing period has ended or is coming close to its end, the registration window will be opened so that you can enter a new license key. For more information, refer to *Registering BitDefender Antivirus for Mac* (p. 48).
- If the malware signatures are outdated, an update will be performed immediately in the background.

- If your system has not been scanned after the installation or for more than 6 days, a scan will be started immediately. The scan wizard will guide you through the scanning process. For more information, refer to *Scan Wizard* (p. 31).
- If there are unresolved threats, a scan will be started to remove them.

3.2. Antiphishing Protection

Besides antivirus protection, BitDefender Antivirus for Mac also provides protection against online phishing scams. These are attempts to steal personal or financial information (for example, user names and passwords, credit card numbers), using a forged web site, with the purpose of making profits or obtaining other benefits.



Important

Antiphishing protection is only available for Mac OS X version 10.5 or later with:

- Safari 5.0.1 (or higher)
- Firefox 3.5 (or higher)

Whenever you try to visit a web page, BitDefender Antivirus for Mac checks it against an online database of web addresses known to be used for phishing. If the web page is in the database, it is automatically blocked and an alert web page is displayed instead.

If you still want to view the web page, use a different browser; but it is strongly recommended not to submit any information on that page.

The BitDefender antiphishing extensions in Safari and Firefox are updated together with BitDefender Antivirus for Mac. You may need to restart your browser to install the updates.

3.3. Shield

The shield scans automatically the accessed files and documents, as well as the applications and processes running on your system. When an infected object is

detected, it is either cleaned or moved to quarantine. In this way, you are protected in real time against malicious software.



Note

Within the computer security industry, the shield is also known as real-time or resident protection, or on-access scanning.

If enabled (default setting), the shield runs in the background, regardless of whether the application is open or not.

3.3.1. Enabling or Disabling Shield

The shield is enabled by default to keep malicious software away from your system. You can disable the shield if you need to, but it is recommended that you turn it on as soon as possible.

To enable or disable real-time protection against malicious software:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Shield** button.
3. Click **ON** or **OFF**.

3.3.2. Configuring Shield Settings

You can configure the real-time protection settings to better suit your needs. Refer to the following topics:

- *Actions Taken on Infected and Suspicious Files* (p. 26)
- *Notifications When Malware Is Found* (p. 26)
- *Archive Scanning Settings* (p. 27)
- *General File Scanning Settings* (p. 28)

Actions Taken on Infected and Suspicious Files

BitDefender Antivirus for Mac automatically tries to clean the infected files it detects. If an infected file cannot be cleaned, it is sent to quarantine. Suspicious files are automatically sent to quarantine.



Important

You should not change the recommended actions unless you have a strong reason to do so.

To change one of the default actions:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Shield** button.
3. Click the corresponding button and choose the desired action. The following actions are available:
 - **Disinfect** - removes the malicious code from the infected file.
 - **Move to quarantine** - moves the infected or suspicious file to quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.
 - **Deny access and notify** - blocks access to the infected file, notifying you about the detected malware through a virus alert.
 - **Delete** - removes the infected or suspicious file from the disk.

Notifications When Malware Is Found

When the shield detects an infected or suspicious file, an alert is displayed. Moreover, when you open the main window, the **Threats** tab is shown automatically to draw your attention to the existing issues.

To change any of these settings:

BitDefender Antivirus for Mac

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Open the Preferences window in one of the following ways:
 - Press the Command key and the Comma key.
 - Click **BitDefender** in the upper-left corner of the screen and choose **Preferences**.
3. Click the **Shield** tab.
4. Select or clear the corresponding check boxes, as needed.

Archive Scanning Settings

BitDefender Antivirus for Mac does not scan accessed archives by default. Scanning archives can slow down your system.

To scan archives automatically on access:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Open the Preferences window in one of the following ways:
 - Press the Command key and the Comma key.
 - Click **BitDefender** in the upper-left corner of the screen and choose **Preferences**.
3. Click the **Shield** tab.
4. Select the **Scan compressed files** check box.
5. Specify the maximum size of the archives to be scanned (in megabytes) in the corresponding field. Archives exceeding the specified size limit will not be scanned. If you want to scan all archives, regardless of their size, type 0.

If you later want to disable the automatic scanning of archives, just clear the check box.

General File Scanning Settings

To speed up scanning, BitDefender Antivirus for Mac checks for malware only files that have not been scanned before or have been modified since their last scan.

To scan all files, even if they have not been modified since their last scan:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac (p. 13)*.
2. Open the Preferences window in one of the following ways:
 - Press the Command key and the Comma key.
 - Click **BitDefender** in the upper-left corner of the screen and choose **Preferences**.
3. Click the **Security** tab.
4. Clear the corresponding check box.

3.3.3. Checking Shield Activity

To check the recent activity of the shield (what files have been scanned and what threats have been detected):

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac (p. 13)*.
2. In the Advanced Controls area of the main window, click the **Shield** button.
3. Depending on the information you need, do any of the following:
 - To see the scanned files log, click **Statistics**.
 - To see the log of the infected files detected, click **Threats**.

3.4. Scanner

This feature allows you to scan specific files or folders on-demand.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned.

You can schedule scan tasks in order to create automatic scanning routines.



Why Is On-demand Scanning Important?

If real-time protection is enabled, BitDefender Antivirus for Mac scans every file you open or copy to the system. If the file is found infected, the application removes or blocks the infection. However, for greater protection, it is recommended to scan your Mac at least once a week.

3.4.1. Scanning Your Mac

You can scan your Mac or specific files anytime you want.

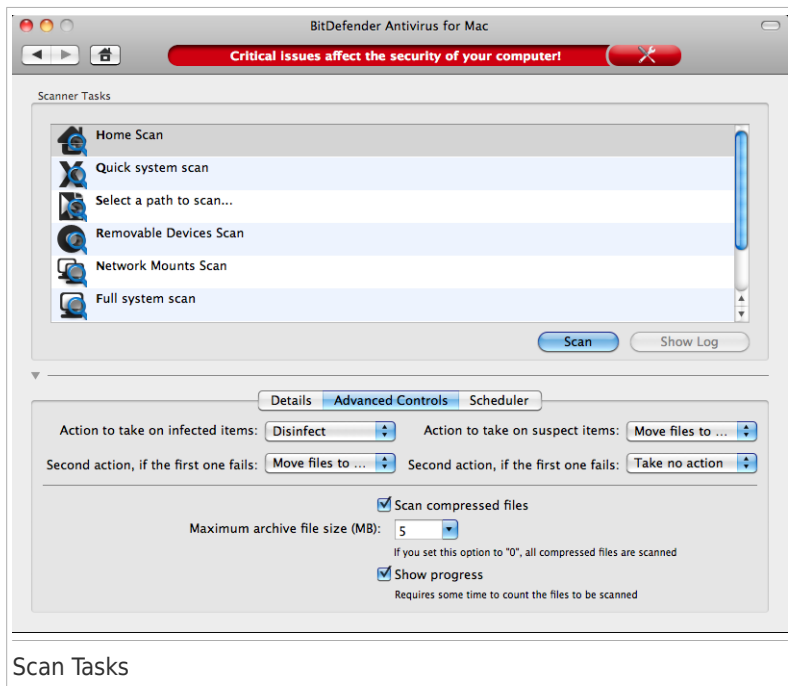
The easiest way to scan a file, a folder or a volume is to drag&drop it over the BitDefender Antivirus for Mac window or Dock icon. The Antivirus Scan wizard will appear and guide you through the scanning process.

For more complex scans, you can use the preconfigured scan tasks.

To start a preconfigured scan:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Scanner** button.
3. Double-click the desired scan task from the list. Alternatively, you can click the scan task and click **Scan**.

BitDefender Antivirus for Mac



You can use the following scan tasks:

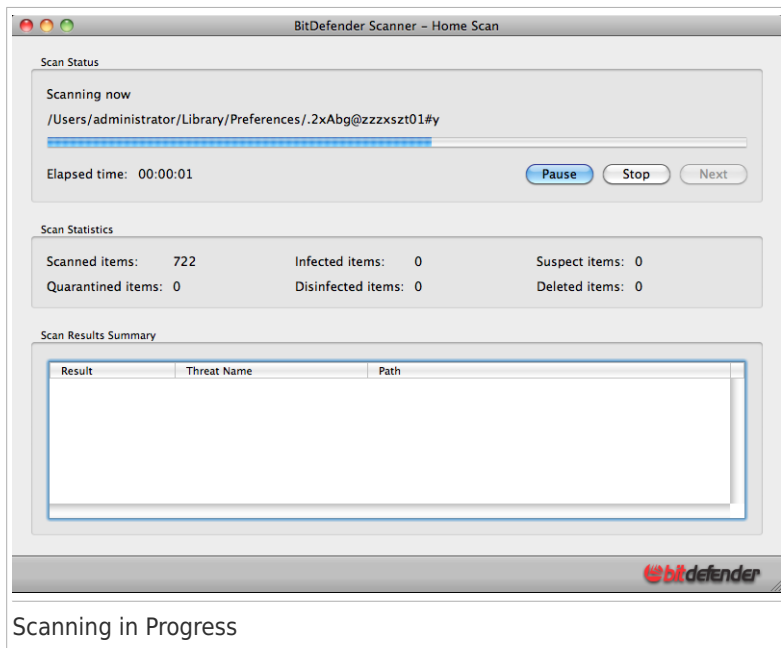
- **Home scan** - checks your home folder for malware.
- **Quick system scan** - checks for malware the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).

- **Select a path to scan** - helps you check specific files, folders or volumes for malware. This task is also used when you scan files by drag&drop.
- **Removable devices scan** - checks for malware all removable drives connected to your Mac (external hard-disks, USB storage devices, CDs/DVDs).
- **Network mounts scan** - helps you check all mounted volumes for malware.
- **Full system scan** - performs a comprehensive check for malware of the entire system.
- **Security issue** - checks for malware only the files that have been detected as infected but on which no action has been taken. This task is used when you fix the detected security issues from the main window.
- **Processes scan** - checks for malware the processes running on your system and the files they access.

3.4.2. Scan Wizard

Whenever you initiate an on-demand scan, the BitDefender Antivirus Scan wizard will appear.

BitDefender Antivirus for Mac



You can see real-time information about the scan. Detected threats and the action taken on them are displayed in the Scan results section.

Wait for BitDefender to finish scanning.

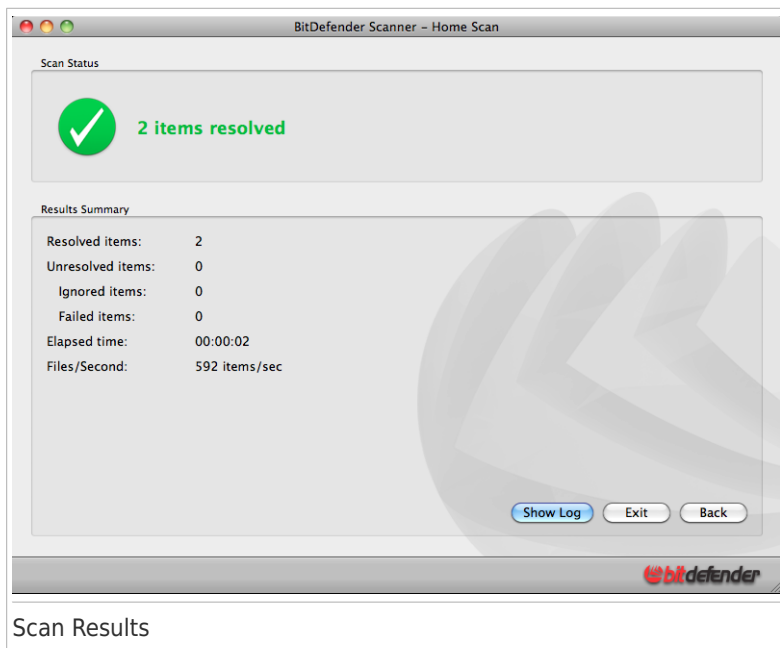


Note

The scanning process may take a while, depending on the complexity of the scan.

Stopping or pausing the scan. You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

When the scanning is completed, a new window will appear, where you can see the scan results.



You can see the results summary. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.

Click **Exit** to close the window.

3.4.3. Checking Scan Logs

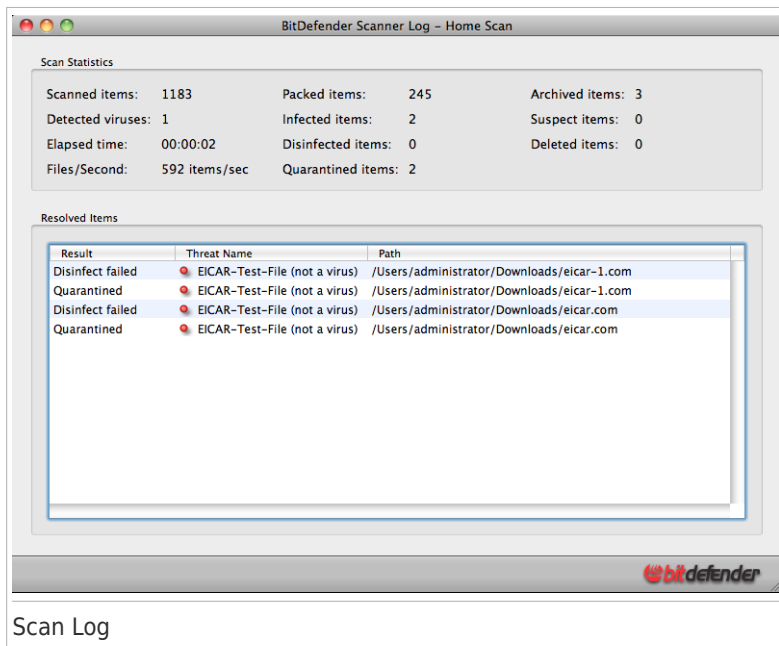
Scan logs provide useful information on the scan.

You can open the scan log directly from the scan results window by clicking **Show Log**.

To check the last scan log of a specific scan task:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac (p. 13)*.
2. In the Advanced Controls area of the main window, click the **Scanner** button.
3. Click the desired scan task from the list. To check the results of the last drag&drop scanning, click **Select a path to scan**.
4. Click **Show Log**.

BitDefender Antivirus for Mac



The screenshot shows the BitDefender Scanner Log window for a Home Scan. It displays scan statistics and a list of resolved items.

BitDefender Scanner Log - Home Scan

Scan Statistics

Scanned items:	1183	Packed items:	245	Archived items:	3
Detected viruses:	1	Infected items:	2	Suspect items:	0
Elapsed time:	00:00:02	Disinfected items:	0	Deleted items:	0
Files/Second:	592 items/sec	Quarantined items:	2		

Resolved Items

Result	Threat Name	Path
Disinfect failed	EICAR-Test-File (not a virus)	/Users/administrator/Downloads/eicar-1.com
Quarantined	EICAR-Test-File (not a virus)	/Users/administrator/Downloads/eicar-1.com
Disinfect failed	EICAR-Test-File (not a virus)	/Users/administrator/Downloads/eicar.com
Quarantined	EICAR-Test-File (not a virus)	/Users/administrator/Downloads/eicar.com

Scan Log

You can see the scan statistics, the resolved items and the action taken on them, and the unresolved items.

3.4.4. Setting Up Scheduled Scans

You can set up scheduled scans to make sure that your system is regularly checked for malware. Set the start time when you know or think your Mac will be on.

To set up a scheduled scan:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Scanner** button.
3. In the list of scan tasks, click the one that you want to schedule. For example, to schedule a comprehensive scan of your Mac, select **Full system scan**.
4. Click **Scheduler**.
5. Select the **Schedule task** check box.
6. Click the button next to **Schedule task** and select the scan frequency: daily, weekly or monthly.
7. Set the start date in the first field. You can type a date or select one using the calendar.
8. In the second field, set the time of the day when the scan should start. You can type the time or set it using the calendar.

3.4.5. Configuring Scan Settings

The settings of the predefined scan tasks are configured for optimal detection and protection. For specific purposes, however, you might want to change the scan settings.

To access the settings of a specific scan task:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Scanner** button.
3. In the list of scan tasks, choose the one the settings of which you want to configure. To configure the settings of drag&drop scanning, click **Select a path to scan**.
4. Click **Advanced Controls**. You can configure the actions taken on the infected and suspicious files detected and other general settings.

Actions Taken on Infected and Suspicious Files

You can configure the following actions:

- **Disinfect** - removes the malicious code from the infected file.
- **Move to quarantine** - moves the infected or suspicious file to quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.
- **Take no action** - only keeps a record of the infected or suspicious file in the scan log. Infected files are regarded as a security issue. You will be notified of their existence in the **Security** tab of the main window.
- **Delete** - removes the infected or suspicious file from the disk.

Other Settings

You can configure the following settings as needed:

- **Scan compressed files.** Select this check box in order to check for malware the compressed files (archives) in the scan locations.

Specify the maximum size of the archives to be scanned (in megabytes) in the corresponding field. Archives exceeding the specified size limit will not be scanned. If you want to scan all archives, regardless of their size, type 0.

- **Show progress.** Select this check box if you want to see an estimate of the remaining scanning time in the scan window. This adds some time to the overall scanning time, but it might be useful for longer scans, such as a **Full system scan**.

3.5. Scan Exclusions

If you want to, you can set BitDefender Antivirus for Mac not to scan specific files, folders, or even an entire volume. For example, you might want to exclude from scanning:

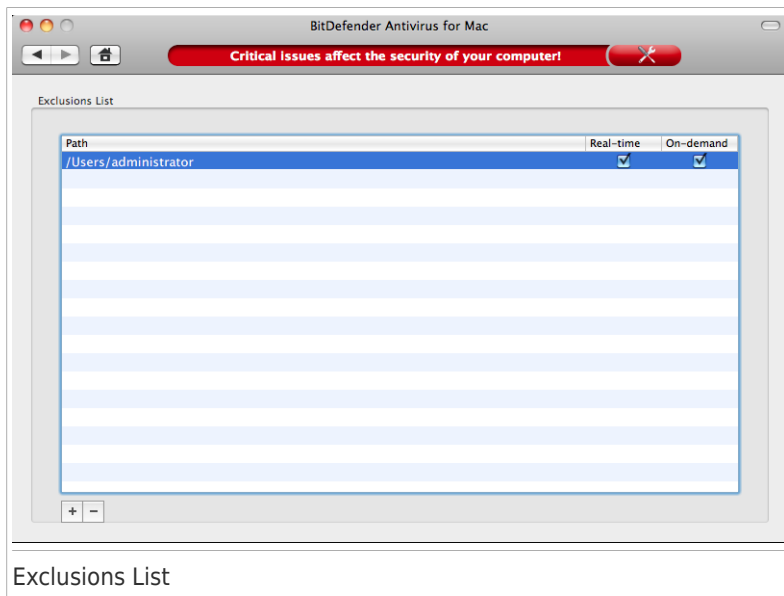
- Backup volumes, because their content is scanned when the backup is performed
- Files that are mistakenly identified as infected (known as false positives)
- Files that cause scanning errors

3.5.1. Accessing the Scan Exclusions List

To set and manage scan exclusions:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Exclusions** button.

3.5.2. Managing Scan Exclusions



The exclusions list contains the paths that have been excluded from scanning. There are two ways to set a scan exclusion:

- Drag&drop a file, folder or volume over the exclusions list.
- Click the button labeled with the plus sign (+), located under the exclusions list. In the new field that appears in the exclusions list, enter the path to the file, folder or volume to be excluded from scanning.

By default, the exclusion will apply to both real-time and on-demand scanning. To apply the exclusion to real-time scanning only, clear the corresponding check box from the **On-demand** column. To apply the exclusion to on-demand scanning only, clear the corresponding check box from the **Real-time** column.

To remove a scan exclusion, select it from the list and click the button labeled with the minus sign (-), located under the exclusions list.

3.6. Quarantine

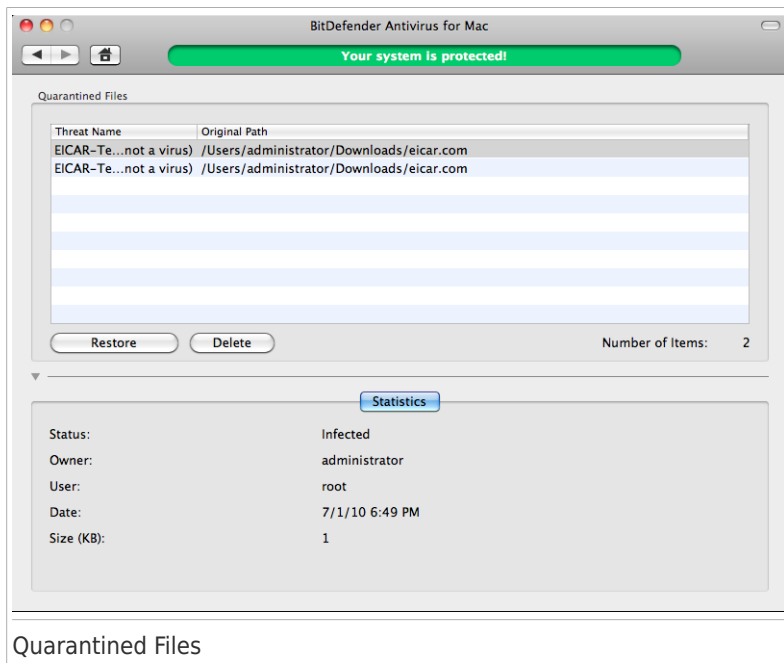
BitDefender allows isolating the infected or suspicious files in a secure area, named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

3.6.1. Accessing Quarantined Files

To view and manage the quarantined files, open the Quarantined files pane:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Quarantine** button.

3.6.2. Managing Quarantined Files



The Quarantine section displays all the files currently isolated in the Quarantine folder.

To delete a file from quarantine, select it and click **Delete**. If you want to restore a quarantined file to its original location, select it and click **Restore**.

3.7. Updates

Updates can be grouped into two categories:

- **Updates to the malware signatures** - enable BitDefender Antivirus for Mac to protect you against the latest malicious software discovered. The BitDefender lab usually releases new malware signatures every hour or even more often.
- **Application updates** - improve the application's performance, stability and usability. They are released every once in a while. Application updates include the updates to the antiphishing extensions in Safari and Firefox.

New malware is found and identified every day. This is why it is very important to keep BitDefender up to date with the latest malware signatures.

- If BitDefender Antivirus for Mac is up-to-date, it can detect the latest threats discovered and clean the infected files.
- If BitDefender Antivirus for Mac is not up-to-date, it may be able to detect some of the recent malware as suspicious, but it will not be able to clean the infected files.

If you are connected to the Internet through broadband or DSL, BitDefender takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that.

3.7.1. Enabling or Disabling Automatic Update

BitDefender Antivirus for Mac must update regularly in order to protect you against new malware and it does that automatically **every hour**.

An active Internet connection is required in order to check for available updates and download them.

To enable or disable automatic update:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).

2. In the Advanced Controls area of the main window, click the **Update** button.
3. Click **ON** or **OFF**.

3.7.2. Requesting an Update

You can request an update manually anytime you want. Update by user request is recommended before you start a comprehensive scan.

An active Internet connection is required in order to check for available updates and download them.

To request an update manually:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. In the Advanced Controls area of the main window, click the **Update** button.
3. Click the **Update Now** button.

You can see the update progress and downloaded files.

Alternatively, if BitDefender Antivirus for Mac is open, you can control-click its Dock icon and choose **Update Now**. The update is performed in the background.

3.7.3. Getting Updates through a Proxy Server

BitDefender Antivirus for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the Internet through a proxy server that requires authentication, you must switch to a direct Internet connection regularly in order to obtain application and malware signature updates.

4. Configuring Preferences

This chapter includes the following topics:

- *Accessing Preferences* (p. 44)
- *General Preferences* (p. 44)
- *Shield Preferences* (p. 46)
- *Security Preferences* (p. 47)

4.1. Accessing Preferences

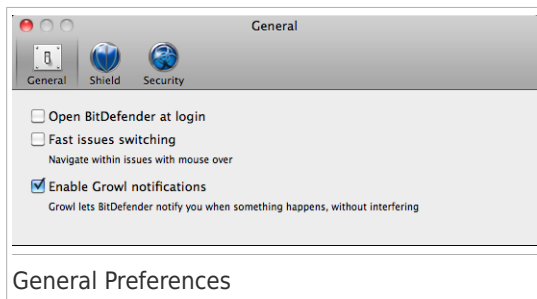
To open the BitDefender Antivirus for Mac Preferences window:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Do any of the following:
 - Click BitDefender in the menu bar and choose **Preferences**.
 - Press Command-Comma(,).

4.2. General Preferences

The general preferences allow you to configure the general behavior of the application.

BitDefender Antivirus for Mac



- **Open BitDefender at login.** Select this check box to open BitDefender Antivirus for Mac automatically when you log in to your account. In this way, you can be notified about current issues and detected malware.



Note

The application is by default minimized in the Dock.

- **Fast issues switching.** Select this check box to navigate through the status panes in the main window with mouse over.
- **Enable Growl notifications.** Select this check box to receive Growl notifications regarding the BitDefender Antivirus for Mac events and activity. You must have Growl installed in order to use this setting.

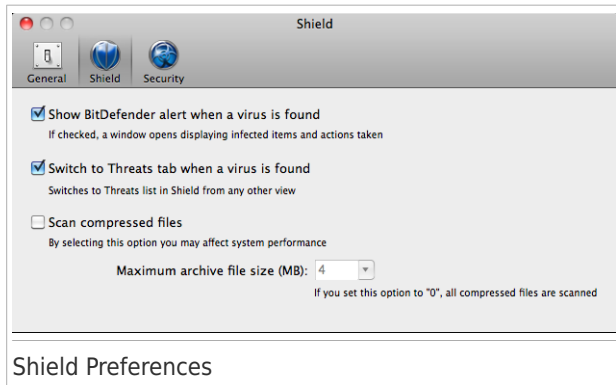


Note

Growl is a third-party application developed by The Growl Project. It is not installed by default on Mac OS X. You can find out more information and download Growl from <http://growl.info/>.

4.3. Shield Preferences

The shield preferences allow you to configure how to be notified about detected malware and the on-access scanning of archives.

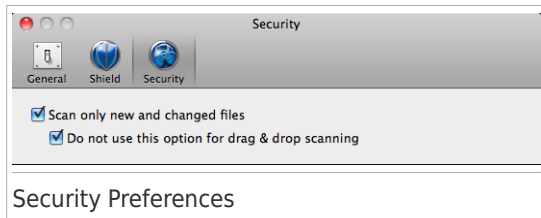


- **Show BitDefender alert when a virus is found.** Select this check box if you want to be notified when a virus or other malware is detected. The alert window displays the infected items and the actions taken on them.
- **Switch to Threats tab when a virus is found.** Select this check box to set BitDefender Antivirus for Mac to directly display the pane of detected threats when you open it.
- **Scan compressed files.** Select this check box if you want to enable on-access scanning of archives. This can slow down your system.

Specify the maximum size of the archives to be scanned (in megabytes) in the corresponding field. Archives exceeding the specified size limit will not be scanned. If you want to scan all archives, regardless of their size, type 0.

4.4. Security Preferences

The security preferences allow you to configure the overall scanning approach.



Scan only new and changed files. Select this check box to set BitDefender Antivirus for Mac to scan only files that have not been scanned before or that have been modified since their last scan.

You can choose not to apply this setting for drag&drop scanning by selecting the corresponding check box.

5. Registering BitDefender Antivirus for Mac

This chapter includes the following topics:

- *About Registration* (p. 48)
- *Registering BitDefender Antivirus for Mac* (p. 48)
- *Purchasing a License Key* (p. 49)

5.1. About Registration

BitDefender Antivirus for Mac comes with 30-day trial period. During the trial period, the product is fully functional and you can test it to see if it meets your expectations.

You must register the product with a license key before the trial period ends. The license key specifies how long you are entitled to use the product. As soon as the license key expires, BitDefender stops performing its functions and protecting your computer.

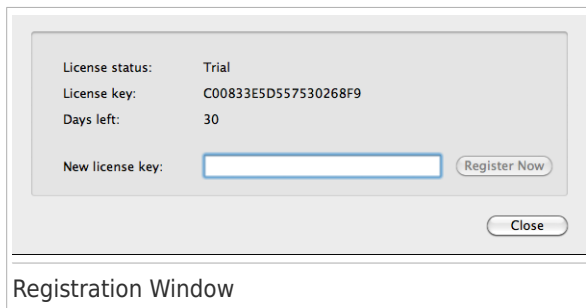
You should purchase a license key or renew your license a few days before the current license key expires.

5.2. Registering BitDefender Antivirus for Mac

An active Internet connection is required in order to register BitDefender Antivirus for Mac.

To register BitDefender Antivirus for Mac:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to *Opening BitDefender Antivirus for Mac* (p. 13).
2. Click **Register Now** in the bottom of the window. The registration window will appear.



The screenshot shows a 'Registration Window' with a light gray background. Inside the window, there is a table-like structure with the following information:

License status:	Trial
License key:	C00833E5D557530268F9
Days left:	30
New license key:	<input type="text"/>

To the right of the 'New license key' input field is a button labeled 'Register Now'. Below the input field and the 'Register Now' button is a 'Close' button. The title 'Registration Window' is at the bottom of the window frame.

3. In the **New license key** field, enter your license key.
4. Click **Register Now** to register your new license.

After the registration is completed, you can see the new registration information in the registration window.

5.3. Purchasing a License Key

When your trial or licensing period comes close to end, purchase a license key to register BitDefender Antivirus for Mac and extend protection.

To purchase a license key:

1. Open BitDefender Antivirus for Mac. If you do not know how to do this, refer to [*Opening BitDefender Antivirus for Mac* \(p. 13\)](#).
2. Click **Buy** in the bottom of the window.
3. Follow the instructions provided in the web page to purchase a license key.

6. Getting Help

This chapter includes the following topics:

- *Support* (p. 50)
- *Contact Information* (p. 52)

6.1. Support

BitDefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your BitDefender product, you can use several online resources to quickly find a solution or an answer. Or, if you prefer, you can contact the BitDefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

6.1.1. Online Resources

Several online resources are available to help you solve your BitDefender-related problems and questions.

- BitDefender Knowledge Base: <http://www.bitdefender.com/help>
- BitDefender Support Forum: <http://forum.bitdefender.com>
- the Malware City computer security portal: <http://www.malwarecity.com>

You can also use your favorite search engine to find out more information about computer security, the BitDefender products and the company.

BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support and development teams, along with more general articles about virus

prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at <http://kb.bitdefender.com>.

BitDefender Support Forum

The BitDefender Support Forum provides BitDefender users with an easy way to get help and to help others.

If your BitDefender product does not operate well, if it cannot remove specific viruses from your computer or if you have questions about the way it works, post your problem or question on the forum.

BitDefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced BitDefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The BitDefender Support Forum is available at <http://forum.bitdefender.com>, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Home & Home Office Protection** link to access the section dedicated to consumer products.

Malware City Portal

The Malware City portal is a rich source of computer security information. Here you can learn about the various threats your computer is exposed to when

connected to the Internet (malware, phishing, spam, cyber-criminals). A useful dictionary helps you understand the computer security terms that you are not familiar with.

New articles are posted regularly to keep you up-to-date with the latest threats discovered, the current security trends and other information on the computer security industry.

The Malware City web page is <http://www.malwarecity.com>.

6.1.2. Asking for Help

In order to ask for help, you must use the BitDefender Web Self-Service. Just follow these steps:

1. Go to <http://www.bitdefender.com/help>. This is where you can find the BitDefender Knowledge Base. The BitDefender Knowledge Base hosts numerous articles that contain solutions to BitDefender-related issues.
2. Search the BitDefender Knowledge Base for articles that may provide a solution to your problem.
3. Please read the relevant article and try the proposed solution.
4. If this solution does not solve your problem, use the link in the article to contact BitDefender Customer Care.
5. Login to your BitDefender account.
6. Contact the BitDefender support representatives by e-mail, chat or phone.

6.2. Contact Information

Efficient communication is the key to a successful business. During the past 10 years BitDefender has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

6.2.1. Web Addresses

Sales department: sales@bitdefender.com

Technical support: <http://www.bitdefender.com/help>

Documentation: documentation@bitdefender.com

Partner Program: partners@bitdefender.com

Marketing: marketing@bitdefender.com

Media Relations: pr@bitdefender.com

Job Opportunities: jobs@bitdefender.com

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Product web site: <http://www.bitdefender.com>

Product ftp archives: <ftp://ftp.bitdefender.com/pub>

Local distributors: <http://www.bitdefender.com/site/Partnership/list/>

BitDefender Knowledge Base: <http://kb.bitdefender.com>

6.2.2. BitDefender Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500

Fort Lauderdale, Florida 33309

Phone (office&sales): 1-954-776-6262

Sales: sales@bitdefender.com

Technical support: <http://www.bitdefender.com/help>

Web: <http://www.bitdefender.com>

BitDefender Antivirus for Mac

Germany

BitDefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland

Office: +49 2301 91 84 222

Sales: vertrieb@bitdefender.de

Technical support: <http://kb.bitdefender.de>

Web: <http://www.bitdefender.de>

UK and Ireland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED

E-mail: info@bitdefender.co.uk

Phone: +44 (0) 8451-305096

Sales: sales@bitdefender.co.uk

Technical support: <http://www.bitdefender.com/help>

Web: <http://www.bitdefender.co.uk>

Spain

BitDefender España SLU

C/ Balmes, 191, 2º, 1ª, 08006
Barcelona

Fax: +34 932179128

Phone: +34 902190765

Sales: comercial@bitdefender.es

Technical support: <http://www.bitdefender.es/ayuda>

Website: <http://www.bitdefender.es>

Romania

BITDEFENDER SRL

West Gate Park, Building H2, 24 Preciziei Street
Bucharest

Fax: +40 21 2641799

Sales phone: +40 21 2063470

Sales e-mail: sales@bitdefender.ro

Technical support: <http://www.bitdefender.ro/suport>

Website: <http://www.bitdefender.ro>

6.2.3. Local Distributors

The BitDefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a BitDefender distributor in your country:

1. Go to <http://www.bitdefender.com/site/Partnership/list/>.
2. The contact information of the BitDefender local distributors should be displayed automatically. If this does not happen, use the Partner Locator tool from the left-side menu to select the area and the country you reside in.
3. If you do not find a BitDefender distributor in your country, feel free to contact us by e-mail at sales@bitdefender.com. Please write your e-mail in English in order for us to be able to assist you promptly.

Types of Malicious Software

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.

What Is Phishing?

In computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from PayPal, eBay, Youtube or online banks are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a web site.

The most common phishing attempts make use of a deceiving e-mail to trick you into submitting personal information on a fake web page. For example, you may receive an e-mail claiming to be from your bank and requesting you to urgently update your bank account information. The e-mail provides you with a link to the web page where you must provide your personal information. Although they seem to be legitimate, the e-mail and the web page the misleading link directs you to are fake. If you click the link in the e-mail and submit your personal information on the fake web page, you will disclose this information to the malicious persons who organized the phishing attempt.

The stolen information is then used to illegally obtain profits or other benefits.